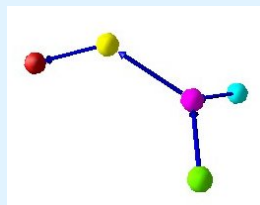


# SANA – Security Analysis in Internet Traffic



4<sup>th</sup> Research Day MINE-Group  
July 2006

Michael Hilker

University of Luxembourg, Campus Kirchberg  
Interdisciplinary Lab for Intelligent and Adaptive Systems  
Management of Information and Net-Centric Computing Group  
6, Rue Richard Coudenhove-Kalergi, L-1359 Luxembourg

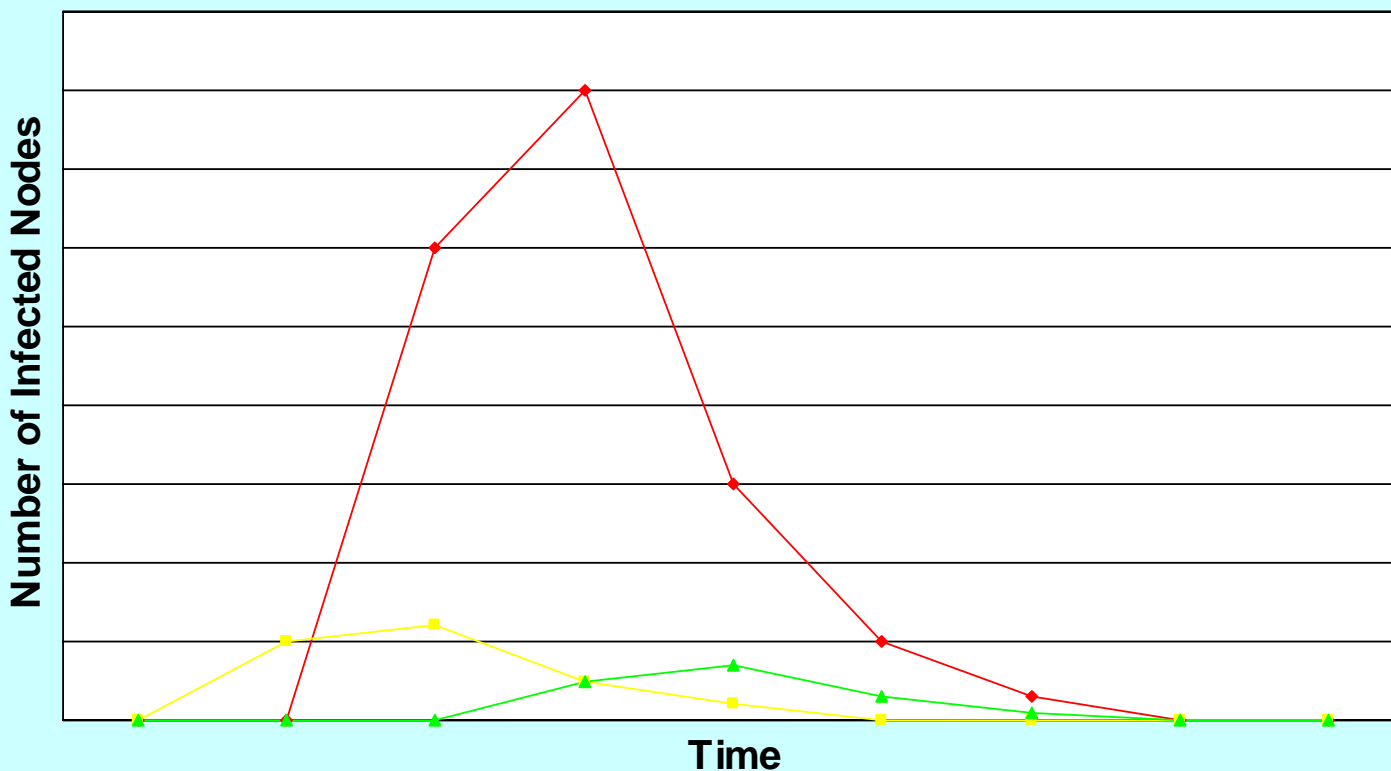
e-mail: [michael.hilker@uni.lu](mailto:michael.hilker@uni.lu) phone: +352-466644-5415

## Network Security – Vision

- Goal: Secure a Network against Attacks
- System should have the following Features:
  - Massively Distributed, Adaptive, Efficient, Autonomous, etc.
  - Similar to the Immune Systems
- The (Immune) System should secure the Network in cooperation with an existing IDS; it should adapt to the current Status of the System (incl. Attacks); it and all components should work autonomously and perform a self-management.

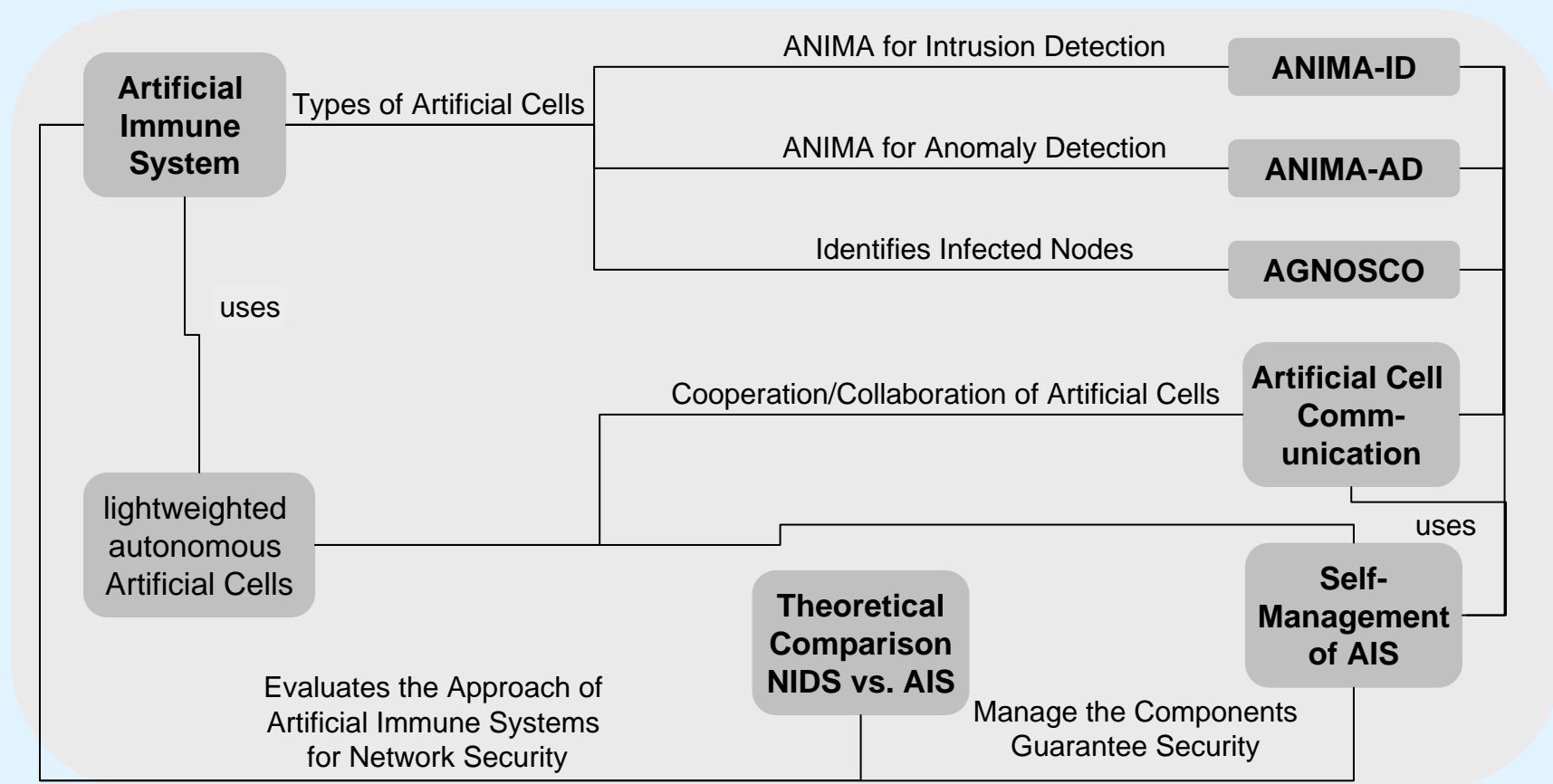
# Network Security – Vision

## Reaction to different Attacks



# SANA – What has been done

SANA



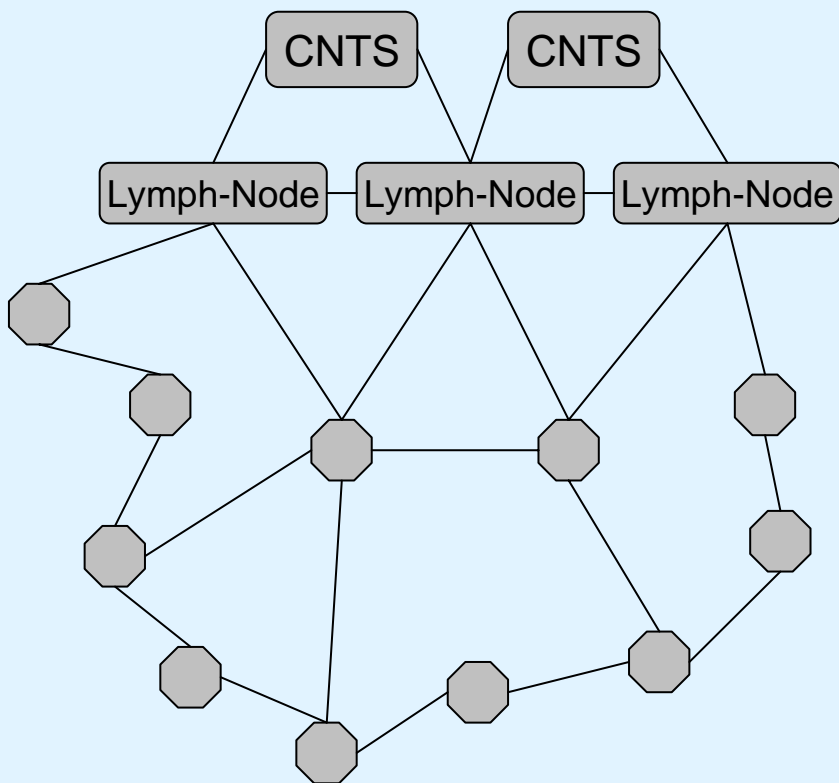
## SANA – Status of the Project

- Second? Prototype is running with Visualization
- Artificial Immune System works
- Artificial Cell Communication is implemented and currently tested
- Different Attack-Scenarios are implemented
- A Worm-Attack is modeled as one Scenario
- First Work in the theoretical Comparison between centralized and distributed IDS is finished

## SANA – artificial Cell Communication

- In SANA, artificial Cells have to cooperate/collaborate like in the Human Body in order
  - to use highly specialized artificial Cells and
  - to reduce false-positives
  
- In SANA, I introduced/implemented an artificial Cell Communication which provides an Infrastructure for the Cell Communication without a central Center.
  
- For this, Structures of the Human Cell Communication are modeled, e.g. Lymph-Nodes, Bone Marrow, etc.

## SANA – Structure of the artificial Cell Communication

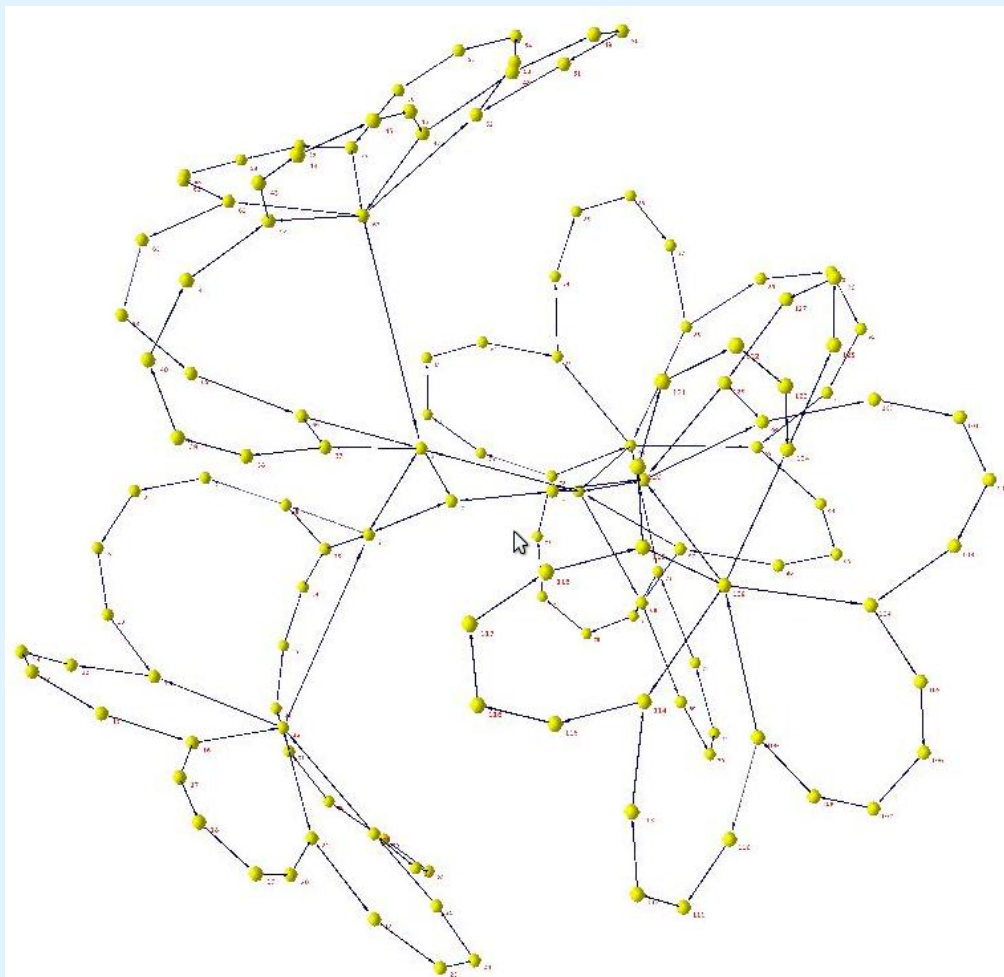


- Network Nodes just know the way to the next Lymph-Nodes.
- Lymph-Nodes supply the artificial Cells and care about the Nodes in a Sub-Sub-Network.
- CNTS supply the Lymph-Nodes and care about the whole Sub-Network. They also release new artificial Cells.
- Communication is done by Substances (Packet with Receptors for right Routing)

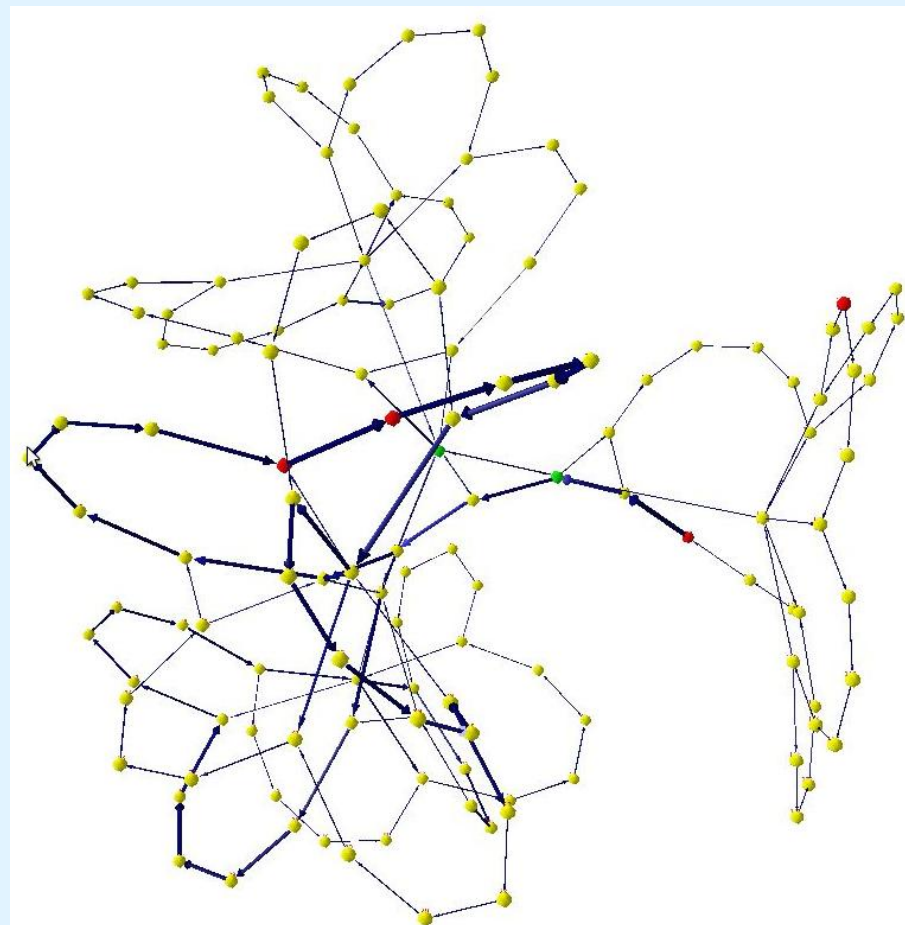
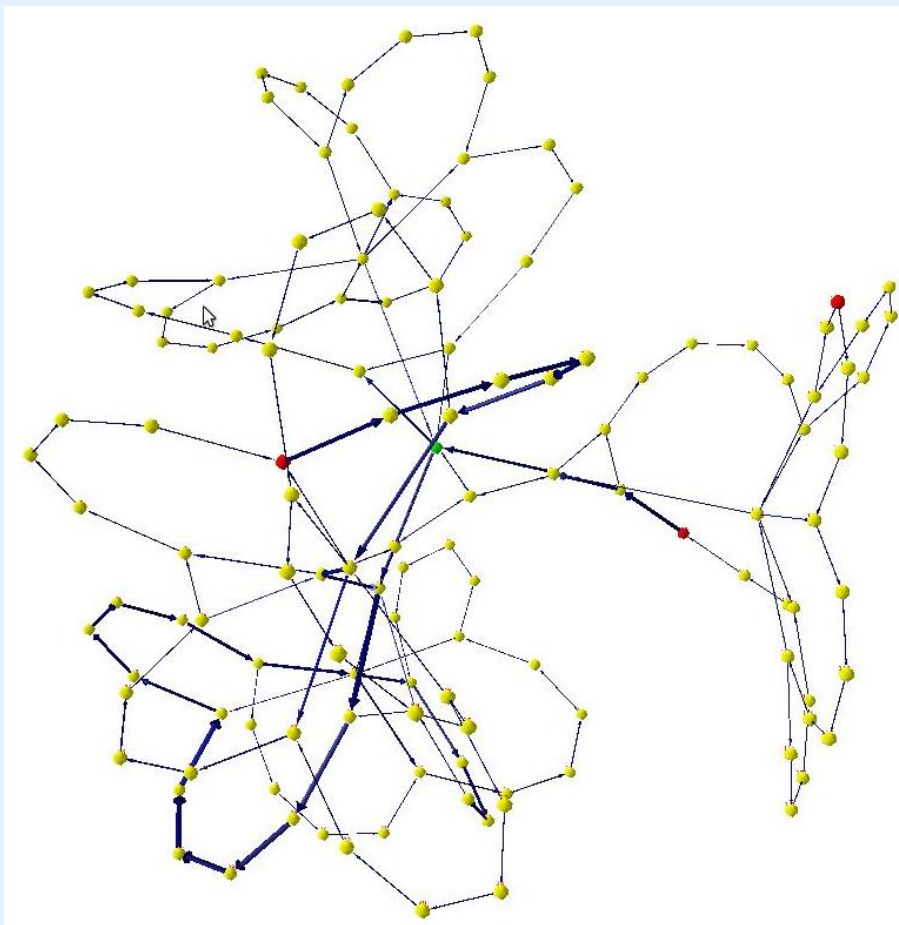
## SANA – Example: Worm Attack

- Definition Worm-Attack:  
A Worm infects a Machine using a Security-Hole and, thereafter, the Worm uses this Machine in order to propagate the Worm in the whole Network and beyond.
- SANA has here three Types of artificial Cells which cooperate:
  - ANIMA-ID: tries to identify Packets containing the Attack
  - AGNOSCO: tries to identify infected Nodes
  - Artificial Cell - Disinfection: disinfects identified infected Nodes
- ANIMA-ID activates a local Immunization so that the Worm is embanked; AGNOSCO identifies the infected Nodes and Artificial Cell-Disinfection uses this Information for Disinfection.

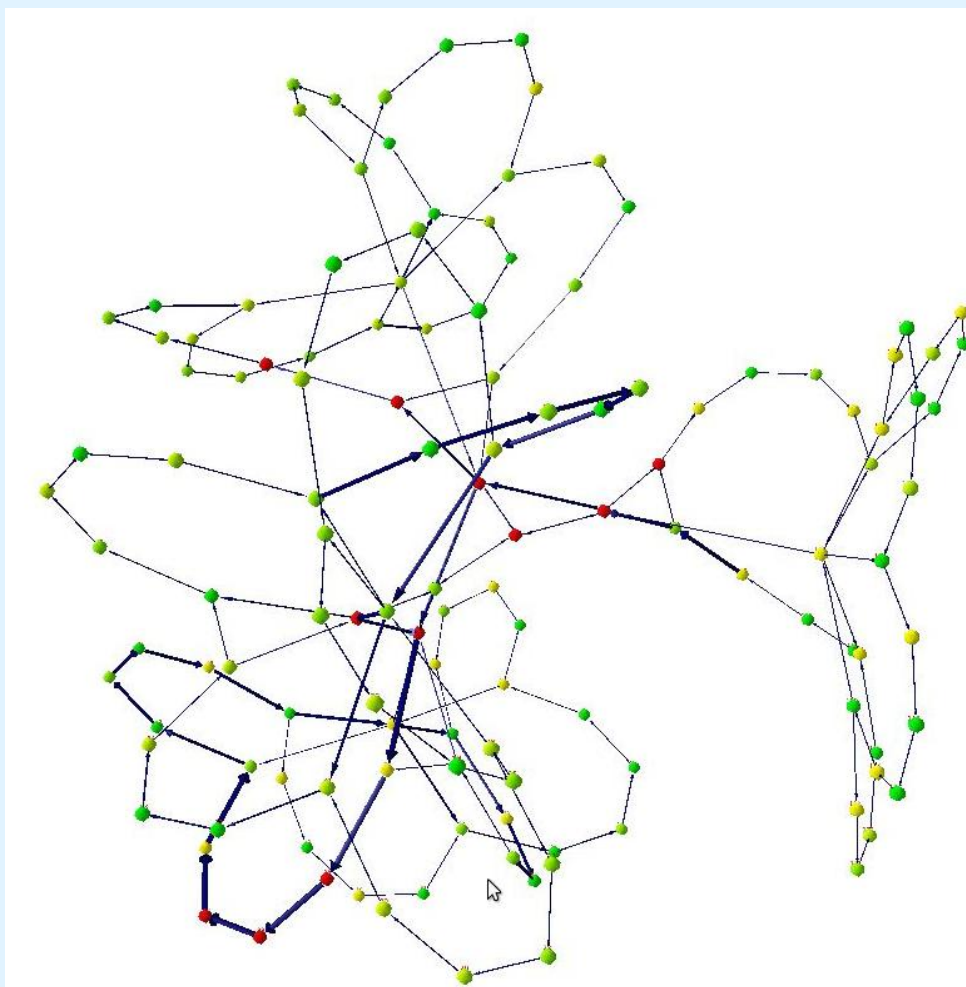
# SANA – Example: Worm Attack



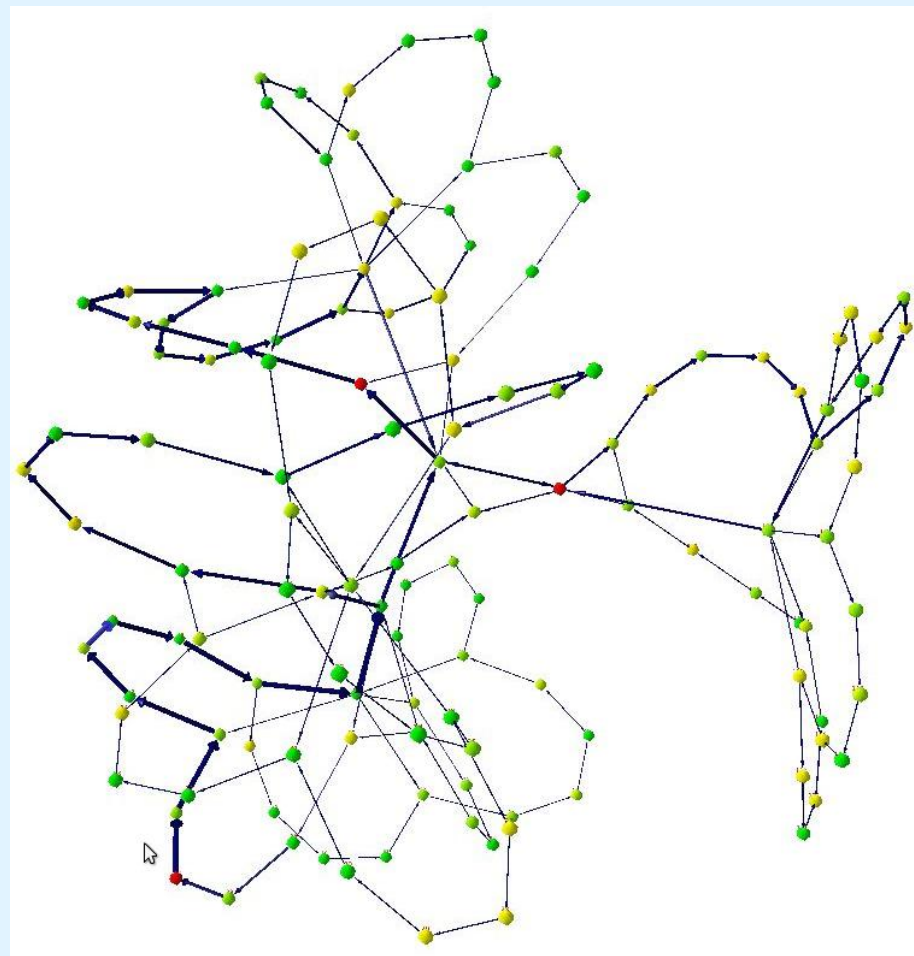
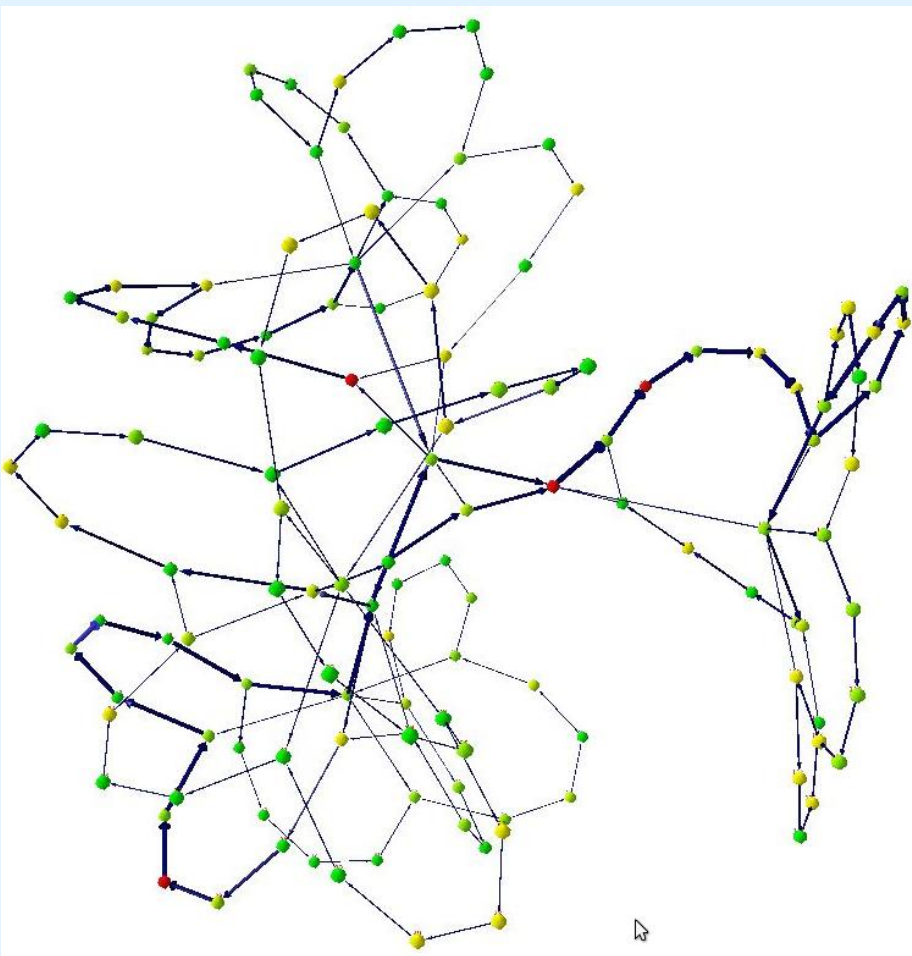
# SANA – Example: Worm Attack



# SANA – Example: Worm Attack



# SANA – Example: Worm Attack



## SANA – Demarcation to other System

- Artificial Cells with the following Attributes
  - Mobile, Lightweighted
  - Autonomous
  - No Usage of a Central Center
  - Massively Distributed System
  
- Artificial Cell Communication
  - Used for the Cooperation and Collaboration of Artificial Cells in order to guarantee certain amount of Security and to increase the Network Security.
  - Use the Cell Regulation and Self-Management Processes for SANA
  
- Modelling of several (not only one or two) Cellular-/Immune-Processes for the Network Security

## SANA – Next Steps

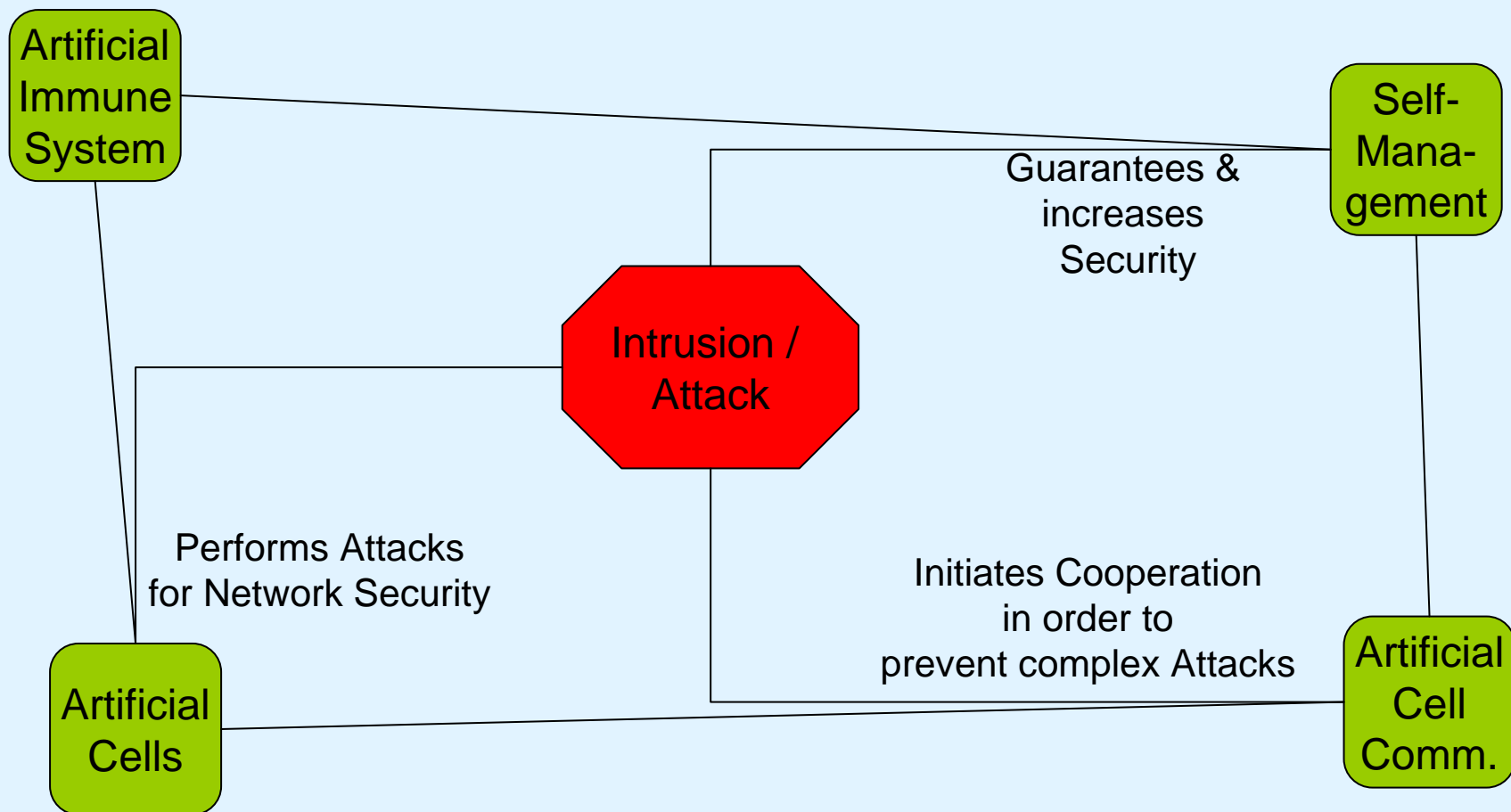
### Research:

- Finish Implementation/Testing artificial Cell Communication
- Increase the Performance of the artificial Cell Communication
- Introduce on top of the artificial Cell Communication a Self-Management of SANA.
- Theoretical Comparison between centralized and distributed IDS
- Write Overview-Article about SANA and publish through Workshop “Trustworthy Software 2006”

# SANA – Self-Management of a massively distributed System

- In the artificial Immune System in SANA, there are lots of specialized, mobile and autonomous artificial Cells. These Entities have to cooperate and they have to organize themselves in order to guarantee the Network Security - one of the main Problems in Multi Agent Systems, Massively Distributed Systems, and Complex Adaptive Systems
- Examples:
  - the artificial Cell should secure all Nodes
    - each Node should have enough artificial Cells
  - the artificial Cells should care about the Resources
    - Cells should distribute over all Nodes
- For this Self-Management, the artificial Cell Communication and novel Structures will be used.

# Conclusion



## Publications

- M. Hilker, C. Schommer: AGNOSCO – Identification of Infected Nodes with artificial Ant Colonies. Proceedings of the 6<sup>th</sup> International Conference on Recent Advances in Soft Computing (RASC2006) July 2006, Canterbury, United Kingdom (to appear).
- M. Hilker, C. Schommer: Description of Bad-Signatures for Network Intrusion Detection. Proceedings, Fourth Australasian Information Security Workshop (AISW-NetSec 2006) during the Australasian Computer Science Week January 2006, Hobart, Australia. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 54.
- M. Hilker, C. Schommer: A new queueing strategy for the Adversarial Queueing Theory. Proceedings, IPSI-2005 December 2005, Bled, Slovenia.
- M. Hilker: Queueing Strategien im Internet Routing. Diploma Thesis at the JW Goethe-University Frankfurt, Germany, March 2005.